Sensing door de politie en PPS

van Noorloos, Marloes

Published in:
Het tijdschrift voor de politie

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Sensing door de politie en PPS: een reflectie

Marloes van Noorloos is universitair docent straf(proces)recht, Universiteit van Tilburg en voorzitter Nederlands Juristen Comité voor de Mensenrechten.

In het voorgaande artikel werd sensing door de politie en de samenwerking met publieke en private partijen door een politiële en politiek-bestuurlijke bril geanalyseerd. In dit artikel wordt de meer wetenschappelijke benadering gevolgd. De immense uitbreiding van de mogelijkheden op dit gebied is bepaald niet zonder risico's. Extra wet- en regelgeving, extra waarborgen en onafhankelijk toezicht zijn de minimale vereisten om die risico's in te dammen.

Wij worden meer en meer omringd door sensoren, die bovendien steeds meer mogelijkheden hebben en steeds dichter bij ons persoonlijke leven komen (Rathenau Instituut 2014). Camera's zullen onze emoties kunnen herkennen en onze identiteit kunnen aflezen aan ons gezicht. Smartphones bevatten steeds meer sensoren: naast gangbare technologie als GPS, microfoon en camera, bijvoorbeeld ook sensoren om temperatuur, lichtsterkte, geluidsintensiteit, bewegingssnelheid en -richting te meten. En er zijn biometrische toepassingen zoals een vingerafdrukscanner. In de nabije toekomst zullen matrassen ons slaapritme monitoren; horloges en T-shirts zullen aan de hand van onze hartslag en huidgeleiding kunnen voorspellen wat ons agressierisico is en of we een psychische stoornis hebben.

Technologische hulpmiddelen zorgen ervoor dat veel meer kan worden waargenomen dan we als mens ooit zouden kunnen. Het is daarmee veel meer dan een gewone versterker van onze zintuigen. Die waarnemingen kunnen bovendien niet los worden gezien van de ultraslimme en snelle analysemogelijkheden die op de verkregen data – in combinatie met enorme hoeveelheden gegevens uit andere bronnen – kunnen worden toegepast.

In al die data kunnen steeds makkelijker patronen en verbanden worden ontdekt en op basis daarvan kunnen geavanceerde profielen worden gemaakt en vervolgens weer toegepast. Die analyse kan zien op data uit het verleden, maar kan ook steeds makkelijker *realtime* worden gemaakt en toegepast. De echte revolutie van 'big data' zit in de voorspellende functie: in de data wordt gezocht naar afwijkende patronen aan de hand waarvan kan worden voorspeld welke personen of groepen een grotere kans hebben om crimineel gedrag te vertonen en op welke locaties de meeste misdrijven kunnen worden verwacht (WRR 2016).

> ***» Op welke manier maakt de politie gebruik van de sensordata?***

Implicaties

Vroeger waren data-analyses gebaseerd op vooraf geformuleerde hypotheses, gebaseerd op gegevens uit het verleden (bijvoorbeeld het gegeven dat eerdere schulden een risico kunnen opleveren voor kredietwaardigheid), en daarbij werd belang gehecht aan het mogelijke causale verband tussen die variabelen. Maar met de enorme hoeveelheden data die we nu tot onze beschikking hebben, kunnen we ook zonder hypotheses en zonder ons zorgen te maken over het *waarom* van correlaties, spontaan op zoek gaan naar geavanceerde patronen die voorspellingen mogelijk maken (Mayer-Schönberger en Cukier 2013). Het bekendste voorbeeld is dat het invoeren van bepaalde zoektermen in Google een sterke indicator is voor griepgevallen (terwijl die zoektermen zelf niets met griep te maken hebben).[1]

Bovendien zijn slimme analysesystemen meer en meer zelflerend: algoritmen kunnen zichzelf aanpassen op basis van feedback. Ze kunnen zelfs worden ingezet om zelfstandig preventief in te grijpen (Hildebrandt 2016; Moerel en Prins 2016) – zonder dat er een mens aan te pas komt kan het computersysteem bepalen dat je op een *no-fly list* komt of dat je geen lening krijgt.

Kortom: het gebruik van sensingtechnologie in het algemeen door de politie kan niet los worden gezien de *manier waarop* de politie gebruikmaakt van de verkregen sensordata en hoe daar vervolgens naar wordt *gehandeld*. Als big data bijvoorbeeld worden gebruikt om te zorgen dat de politie-inzet meer wordt gefocust op bepaalde wijken, zitten mogelijke problemen vooral in de indirecte discriminatie die dat kan veroorzaken en de *selffulfilling prophecy* die daarmee wordt gecreëerd (een wijk krijgt meer aandacht, dus vind je er ook meer incidenten en dat vertaalt zich weer in de criminaliteitscijfers die vervolgens in het systemen worden gezet).

Stratumseind

Een ander soort toepassing is het sturen van wat extra politie-inzet naar een plaats waar *realtime* data-analyse laat

zien dat er mogelijk openbare-ordeverstoringen op de loer liggen – zoals in het project Stratumseind (CityPulse) in Eindhoven dat ook in het vorige artikel wordt genoemd. Het gaat hier om een handhavend optreden in de openbare ruimte, waarbij de handeling – extra politie-inzet – op zichzelf weinig ingrijpend is.

Wat hier echter wel problematisch kan zijn, is de massale surveillance van onschuldige burgers – vanuit een veelheid aan private en publieke bronnen – die er aan ten grondslag ligt. Daarbij gaat het bijvoorbeeld ook om camera's die eigenlijk bedoeld zijn voor andere doelen zoals het managen van verkeersstromen, en om mobiele telefoongegevens van het uitgaanspubliek. Dat zal zich nauwelijks bewust zijn van het feit dat deze gegevens door de politie kunnen worden afgelezen.

Ook in de openbare ruimte mogen we een redelijke privacy-verwachting hebben, zeker wanneer camera's in die publieke ruimte zeer persoonlijke informatie over onze emotionele gesteldheid kunnen prijsgeven. En wat als de politie in de toekomst ook hartslag- en vochtsensoren uit onze *smartwatch* kan meenemen in dit systeem (waarvoor we ooit gedachteloos een toestemmingsvinkje blijken te hebben aangekruist)?

In het voorbeeld van CityPulse is daarom wel gezorgd dat de gegevens in het systeem niet herleidbaar zijn tot individuen, wat tegenwoordig wel specifieke actie vergt omdat het combineren van datasets juist tot hernieuwde identificatie kan leiden (Van de Nieuwenhof 2015). Ook was er geen sprake van automatische beslissingen; de politie bepaalde of actie nodig was.

Proportionaliteit

Toch blijft er iets ongemakkelijks kleven aan het idee van een zelflerend systeem dat zoekt naar 'afwijkende patronen' in het gedrag van (groepen) mensen, en op basis daarvan voorspellingen doet over de toekomstige misdrijven die zij zouden kunnen plegen. Natuurlijk, systemen worden steeds intelligenter en verkeerde voorspellingen (zoals het verwarren van een *flashmob* van twee tegenover elkaar dansende groepen, met een potentiële vechtpartij (Rathenau Instituut 2015)) kunnen daarmee steeds beter worden voorkomen. Maar de vraag is uiteindelijk: willen we naar een maatschappij waarin zelflerende systemen ons continu surveilleren op 'abnormaal gedrag' zodat kan worden ingegrepen voordat er iets gebeurt? Voor wat voor soort misdrijven is het proportioneel om zo'n middel in te zetten?

Die vraag wordt des te prangender als op basis van dergelijke statistische voorspellingen over geweldgebruik, individuele personen op de korrel worden genomen voor verdere controle, terwijl ze nog geen strafbaar feit hebben gepleegd. Daarbij is essentieel dat de uitkomst van een analyse met menselijke tussenkomst en nadere bevestigende informatie moet worden gevalideerd. Pas dan zou het tot een verdenking en eventueel tot de inzet van dwangmiddelen mogen leiden (zie ook Brinkhoff 2014 en 2016).

Methodiek

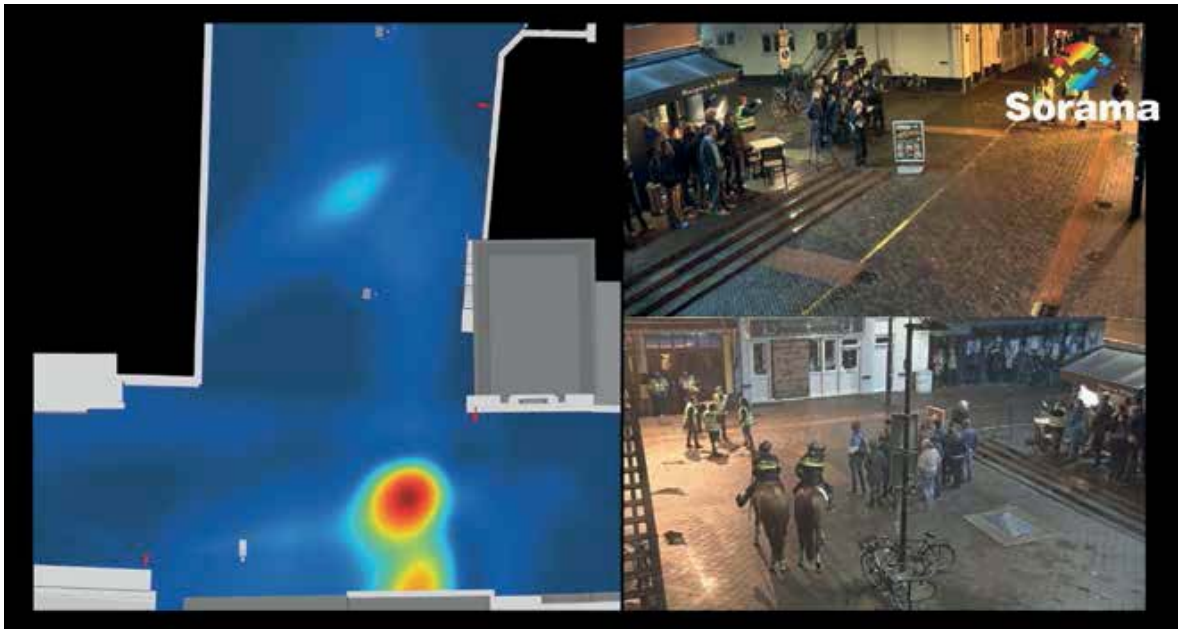
Wat tevens van belang is, is hoe de voorspelling tot stand komt: op basis van relevante informatie uit het verleden en/of goed gegronde hypotheses, of op basis van willekeurige correlaties ('mensen met een blauwe jas en rood haar hebben rond half 1 's nachts een grotere kans om geweld te plegen en die houden we dus extra goed in de gaten')? In dat laatste geval kom je bij toeval in een risicogroep terecht zonder dat daar een gegronde reden voor is.

Als de politie bijvoorbeeld in het kader van het voorkomen van ladingdiefstallen afgaat op voertuigen die veelvuldig binnen een korte periode worden gesignaleerd bij bepaalde parkeerplaatsen, ligt daar in elk geval een logisch te verdedigen voorspeller aan ten grondslag (en een concreet veiligheidsprobleem waar gericht op gereageerd kan worden). Zo is ook het zoeken naar ANPR-hits met referentiebestanden van bekende overvallers of inbrekers in specifieke gebieden beter te verdedigen dan algemene *fishing expeditions*.

Een bijeffect van dit soort methoden is dat categorieën mensen die intensiever in de gaten worden gehouden, logischerwijs ook sneller op het plegen van een strafbaar feit worden betrapt. Het systeem kan daarmee bevooroordeeld raken (WRR 2016). Bovendien: als je op basis van onbekende algoritmen zou worden verdacht, wat kun je daar dan tegen inbrengen? Er is weliswaar aandacht voor transparantie over zulke algoritmen, maar ze zijn vaak extreem ingewikkeld en bovendien als gesteld zelflerend (Moerel en Prins 2016).

Het blijft dus van belang om te onderkennen dat het altijd gaat om waarschijnlijkheden en niet om zekerheden, en dat er fouten in het systeem kunnen sluipen (Hildebrandt 2016), zeker wanneer veel verschillende datasets worden gecombineerd. Sommige gebeurtenissen, zoals terroristische aanslagen, komen (gelukkig) zo weinig voor dat patroonherkenning niet goed te doen is (Schneier 2015).

Wanneer gebruik wordt gemaakt van de data van private bedrijven of personen, worden de mogelijkheden van *sensing* enorm. Zeker omdat dataverzameling voor private bedrijven tegenwoordig niet zomaar een bijproduct meer is, maar een businessmodel op zichzelf (Moerel en Prins 2016).



3D City Sound Camera's van Sorama pikken afwijkende geluiden op op het Stratumseind, november 2015.

Wanneer de politie die data gebruikt – evenals data van andere overheidsinstellingen zijn die soms weer gebaseerd op data van private bedrijven – brengt dit bijzondere risico's met zich mee. Daarom zijn er afspraken nodig over wie bij zo'n samenwerking verantwoordelijk is voor de betrouwbaarheid en rechtmatigheid van de verwerking van de gegevens (Brinkhoff 2014). Wat als verouderde of onjuiste informatie nog steeds in de bestanden is opgenomen, zoals bij ANPR-referentiebestanden weleens het geval was? (Flight en Van Egmond 2011, p. 51).

Wantrouwen en machtsonbalans

Kortom: enerzijds is het soort gebruik dat de politie maakt van sensordata van groot belang voor de vraag of het juridisch-ethisch verdedigbaar is. Anderzijds is essentieel dat de omvang en frequentie van surveillance beperkt blijft. Zeker nu de openbare en de intieme sfeer steeds dichter bij elkaar komen en de hoeveelheid sensoren enorm toeneemt. Dat mensen deze technologie zelf ook in toenemende mate gebruiken, is niet doorslaggevend: de politie moet zelf heel duidelijk aantonen waarom het noodzakelijk en proportioneel is om sensing toe te passen. De politie heeft immers ook vergaande machtsmiddelen tot haar beschikking én heeft de mogelijkheden om sensing-data te combineren met veel andere databestanden.

Het gevaar bestaat anders dat uiteindelijk iedereen als potentieel veiligheidsrisico of zelfs als potentiële verdachte wordt gezien in plaats van als vrije burger (en dat we elkaar ook zo gaan zien). Zo ontstaat een maatschappij gebaseerd op wantrouwen van iedereen die zich niet 'normaal' gedraagt (Van Brakel en De Hert 2011). Hoe meer we weten over veiligheidsrisico's, hoe meer we ze ook willen inperken en hoe meer we dus willen weten – een vicieuze cirkel (Vis 2012:149). De WRR heeft daarnaast gewezen op het gevaar van een machtsonbalans wanneer burgers steeds transparanter worden voor de overheid, terwijl er andersom veel geheimzinnigheid is over de profielen en algoritmen die overheidsinstanties gebruiken om burgers te controleren (WRR 2016).

Wet- en regelgeving

Nemen we alle nieuwe en toekomstige mogelijkheden in ogenschouw, dan is het sterk de vraag of de huidige wetgeving nog voldoende privacywaarborgen biedt en of de algemene grondslag van artikel 3 Politiewet voldoende is. Omdat het gaat om zulke vergaande surveillancemogelijkheden die aan de samenleving als geheel raken, is het van groot belang dat hierover expliciet in een democratisch proces wordt beslist en dat het maatschappelijk middenveld daarbij betrokken wordt. Sommige toekomstige toepassingen van sensortechnologie kunnen al zover gaan dat een speciale wettelijke grondslag daarvoor gewenst is. Daarnaast kunnen de inzet van diverse sensingtechnologieën en het gebruik en de analyse van de daaruit voortvloeiende data niet los van elkaar worden gezien.

Is de tweedeling tussen de regimes van artikel 3 Politiewet – tussen opsporingsmethoden die een geringe privacy-inbreuk maken enerzijds en stelselmatige observatie anderzijds – in het huidige tijdsgewricht niet te zwart-wit? Bij artikel 3 Politiewet komt er in eerste instantie geen officier van justitie of rechter aan te pas en hoeft er geen sprake te zijn van een verdenking. Bij stelselmatige observatie is er sprake van een meer dan beperkte privacy-inbreuk en gelden sterkere waarborgen. Juist vanwege de enorme toepassings- en combinatiemogelijkheden van (sensor)data moeten we die mogelijkheden mijns inziens beschouwen als een meer dan beperkte inbreuk op de *collectieve* privacy, en daarom zijn nadere waarborgen nodig (Mantelero 2016). Voor het beschermen van deze collectieve aspecten biedt het strafrecht momenteel nauwelijks remedies. Onafhankelijke controle in een vroeger stadium is dus van groot belang.

Ook met betrekking tot de bepalingen in het Wetboek van Strafvordering over het vorderen van gegevens van private partijen geldt dat de hoeveelheid en diversiteit aan gegevens enorm is toegenomen en dat daarmee steeds dieper op de persoonlijke levenssfeer kan worden ingegrepen. Uit de dataretentie-uitspraak van het Europese Hof van Justitie[2] (en in navolging daarvan de Nederlandse rechter[3]) blijkt bovendien dat rechterlijke toetsing voor het gebruik van bepaalde gegevens van groot belang is. Zeker als het gaat om data van grote aantallen onschuldige burgers. Ook als wel een verdenkingscriterium geldt, blijken in de praktijk vorderingen tot verstrekking van gegevens aan private partijen soms van beide zijden heel ruim geïnterpreteerd te worden. Zo worden grote gegevensstromen opgeleverd, ook over onschuldige burgers (Janssen 2015).

In horizontale verhoudingen tussen burgers en bedrijven zorgen big data eveneens voor grote uitdagingen voor de privacy. Deze kunnen gemakkelijk doorwerken als de politie gebruik maakt van private gegevens. Individuen weten nauwelijks welke gegevens bedrijven en overheidsinstanties over hen kunnen verzamelen en analyseren door

> *» Essentieel is de rol van onafhankelijk toezicht bij het gebruik van sensing*

middel van groepsprofielen, en welke toegang politie en justitie tot die gegevens hebben.

Extra waarborgen

Een gemoderniseerde wettelijke regeling alleen is niet voldoende. Bij het aangaan van publiek-private samenwerkingsverbanden op het gebied van sensing is *privacy by design* van groot belang. Dit beginsel moet vanaf het beginstadium diep in het systeem zijn ingebouwd (Koops et al 2012). Denk daarbij aan het onherkenbaar maken van gezichten, het verwijderen van gegevens na het verstrijken van de bewaartermijn en *bodycams* die duidelijk maken aan het publiek wanneer ze aan staan (Coudert et al 2015).

Ook op het niveau van algoritmes en zelflerende systemen moeten de waarborgen al vanaf het begin worden ingebouwd. En deze dienen steeds te worden gemonitord, mede om daar transparantie over te kunnen bieden aan burgers en om te zorgen dat er altijd een menselijke factor nodig blijft in het nemen van beslissingen (Koops et al 2012). In een proeftuin kan daar mee geëxperimenteerd worden.

Het inbouwen van waarborgen vanaf het begin is dus cruciaal. Tegelijkertijd moeten we altijd het grotere plaatje in de gaten blijven houden: de overheid zal moeten aantonen waarom het noodzakelijk en proportioneel is om bepaalde toepassingen mogelijk te maken. Ook als een landelijk dekkend sensornetwerk met slimme design-oplossingen 'privacy-proof' is te maken, wil dat nog niet zeggen dat zo'n netwerk geen risico's kan opleveren, nu of in de toekomst.

Essentieel is de rol van onafhankelijk toezicht bij het gebruik van sensing en de daaruit voortkomende data. Die beoordeling zou op verschillende manieren kunnen worden versterkt. Bijvoorbeeld door deze onder supervisie van de toezichthouders door onafhankelijke personen te laten plaatsvinden, daarbij verschillende stakeholders te betrekken en door de sociale en ethische impact van een project te beoordelen (Mantelero 2016).

Bovendien moet na verloop van tijd onafhankelijk en op transparante wijze geëvalueerd worden of het sensing-project het politiewerk daadwerkelijk effectiever heeft gemaakt en welke (neven)effecten het in maatschappelijk opzicht heeft opgeleverd. «

Literatuur

Brakel, R. van en Hert, P. de, 'Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies', *Journal of police studies* 2011, nr. 3, p. 163-192.

Brinkhoff, S., *Startinformatie in het strafproces* (proefschrift RUN), 2014, Wolters Kluwer.

Brinkhoff, S., 'Big datamining door de politie', *Nederlands Juristenblad* 2016, nr. 20, p. 1400-1407.

Coudert, F., Butin, D. en Métayer, D. Le, 'Body-worn cameras for police accountability: opportunities and risks', *Computer law & security review* 2015, p. 749-762.

Est, R. van, m.m.v. V. Rerimassie, I. van Keulen en G. Dorren, 'Intieme technologie: de slag om ons lichaam en gedrag', Den Haag, Rathenau Instituut 2014.

Flight, S. en Egmond, P. van, *Hits en hints. De mogelijke meerwaarde van ANPR voor de opsporing,* 2011, Amsterdam: DSP-groep.

Hildebrandt, M., 'Data-gestuurde intelligentie in het strafrecht', *Preadvies NJV*, 2016, Wolters Kluwer.

Janssen, S.L.J., 'Ongenormeerde opsporing: de wijd openstaande achterdeur van private gegevensvergaring', *Strafblad* 2015, nr. 2, p. 120-126.

Kool, L., Timmer, J. en Est, R. van, *De datagedreven samenleving. Achtergrondstudie*, 2015, Den Haag: Rathenau Instituut.

Koops, E.J., Bodea, G., Broenink, G., Cuijpers, C.M.K.C., Kool, L., Prins, J.E.J. en Schellekens, M.H.M., *Juridische scan openbronnonderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools,* 2012, Tilburg University: TILT.

Lazer, D., Kennedy, R., King, G. en Vespignani, A., 'The parable of Google Flu: Traps in big data analysis', *Science* 2014, p. 1203-1205.

Mantelero, A., 'Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection', *Computer law & security review* 2016, p. 238-255.

Mayer-Schönberger, V. en Cukier, K., *De big data revolutie,* 2013, Amsterdam: Maven Publishing.

Moerel, E.M.L. en Prins, J.E.J., 'Privacy voor de homo digitalis', *Preadvies NJV,* 2016, Wolters Kluwer.

Nieuwenhof, J. van de, 'Een kijkje in het lab van het Stratumseind', 9 september 2015, https://e52.nl/een-kijkje-in-het-lab-van-het-stratumseind/.

Schneier, B., *Data and Goliath: the hidden battles to collect your data and control your world,* 2015, New York: W.W. Norton & Company.

Vis, T. , *Intelligance, politie en veiligheidsdienst: verenigbare grootheden? (proefschrift Tilburg),* 2012.

Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *Big data voor een vrije en veilige samenleving,* 2016, Den Haag: WRR.

Noten

1 Al wordt de waarde van dit voorbeeld inmiddels al weer in twijfel getrokken: Lazer et al 2014.

2 HvJ (GK) Digital Rights Ireland Ltd, 8 april 2014, C-293/12 en C-594/12.

3 Rb Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498.